| Form PTO 1449 (Modified) | U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE | ATTY DOCKET NO. 240527US2SRD DIV | SERIAL NO. 10/660,679 New Application |
|---|---|---|---|
| LIST OF REFERENCES CITED BY APPLICANT | | APPLICANT Shinichi KAWAMURA | |
| | | FILING DATE Herewith  9/12/03 | GROUP 2124 ~~Unassigned~~ |

**U.S. PATENT DOCUMENTS**

| EXAMINER INITIAL | | DOCUMENT NUMBER | DATE | NAME | CLASS | SUB CLASS | FILING DATE IF APPROPRIATE |
|---|---|---|---|---|---|---|---|
| ✓ | AA | 4,996,527 | 02/91 | Houk et al | | | |
| ✓ | AB | 5,050,120 | 9/91 | Houk, Theodore L. | | | |
| ✓ | AC | 5,107,451 | 4/92 | Houk, Theodore L. | | | |
| ✓ | AD | 5,987,487 | 11/99 | Welland, David R. | | | |
| | AE | | | | | | |
| | AF | | | | | | |
| | AG | | | | | | |
| | AH | | | | | | |
| | AI | | | | | | |
| | AJ | | | | | | |
| | AK | | | | | | |
| | AL | | | | | | |
| | AM | | | | | | |
| | AN | | | | | | |

**FOREIGN PATENT DOCUMENTS**

| | | DOCUMENT NUMBER | DATE | COUNTRY | TRANSLATION YES | NO |
|---|---|---|---|---|---|---|
| | AO | | | | | |
| | AP | | | | | |
| | AQ | | | | | |
| | AR | | | | | |
| | AS | | | | | |
| | AT | | | | | |
| | AU | | | | | |

**OTHER REFERENCES (Including Author, Title, Date, Pertinent Pages, etc.)**

| | | |
|---|---|---|
| ✓ | AV | Shinichi KAWAMURA, et al., "COX-ROWER ARCHITECTURE FOR FAST PARALLEL MONTGOMERY MULTIPLICATION," Lecture Notes in Computer Science, No. 1807, May 2000, pgs. 523-538 |
| ✓ | AW | Karl C. POSCH, et al., "MODULO REDUCTION IN RESIDUE NUMBER SYSTEMS," IEEE Transactions on Paralell and Distributed Systems, Vol. 6, No. 5, May 1995, pgs 449-454 |
| ✓ | AX | J. SCHWEMMEIN, et al., "RNS-MODULO REDUCTION UPON A RESTRICTED BASE VALUE SET AND ITS APPLICABILITY TO RSA CRYPTOGRAPHY," Computers and Security, Vol. 17, No. 7, 1998, pgs. 637-650 |
| ✓ | AY | Jean-Claude BAJARD, et al., "AN RNS MONTGOMERY MODULAR MULTIPLICATION ALGORITHM," IEEE Trans. On Computers, Vol. 47, No. 7, pgs, 1998, 766-776 |
| ✓ | AZ | Pascal PAILLIER, "LOW-COST DOUBLE-SIZE MODULAR EXPONENTIATION OR HOW TO STRETCH YOUR CRYPTOPROCESSOR," Lecture Notes in Computer Science, No. 1560, 1999, pgs. 223-234 |

☐ Additional References sheet(s) attached

| Examiner  D. H. Malzahn | Date Considered  9/12/03 |
|---|---|

*Examiner: Initial if reference is considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

I:\ATTY\MM\AMENDMENT\620\240527US-PTO 1449.DOC